<u>IN THE UNITED STATES PATENT AND TRADEMARK OFFICE</u>

In re Application of: Examiner: Peng, Fred H.

    Robert Corrigan and

    Paul Alioshin

Serial No.   09/832,738   Art Unit: 2623

Filing Date: April 10, 2001   Attorney Docket No.: SLM-05800

Title: Method, System and Display Apparatus for Encrypted Cinema

---

Honorable Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

<u>APPEAL BRIEF FILED UNDER 37 C.F.R. § 41.37</u>

Sir:

    This appeal brief follows the Notice of Appeal filed by Applicants on May 21, 2008.

I.   REAL PARTY IN INTEREST

    The real party in interest is Silicon Light Machines Corporation, a California corporation having its principal place of business in San Jose, California.

II.   RELATED APPEALS AND INTERFERENCES

On information and belief, there are no appeals, interferences, or judicial proceedings known to the appellant, the appellant's legal representative, or assignee which may be related to, directly affect or be directly affected by or have a bearing on the Board of Patent Appeals and Interferences (the "Board") decision in the pending appeal.

III.   STATUS OF CLAIMS

    A.   Total Claims: 1-38

    B.   Current Status of Claims:

        1.   Claims canceled: 2-3, 5-6, 9, 15-18, 20-24, and 31-34

        2.   Claims withdrawn: none

        3.   Claims pending: 1, 4, 7-8, 10-14, 19, 25-30 and 35-38

        4.   Claims allowed: none

        5.   Claims rejected: 1, 4, 7-8, 10-14, 19, 25-30 and 35-38

        6.   Claims objected to: none

    C.   Claims on Appeal: 1, 4, 7-8, 10-14, 19, 25-30 and 35-38

As indicated above, claims 1, 4, 7-8, 10-14, 19, 25-30 and 35-38 are pending in this application, stand finally rejected, and are being appealed. These claims are rejected in the final office action mailed January 2, 2008 ("the last office action").

IV.   STATUS OF AMENDMENTS

No amendment has been entered after the final rejection.

V.   SUMMARY OF CLAIMED SUBJECT MATTER

The claimed subject matter relates to video display systems.

Independent claim 1 relates to a method of securely displaying visual data. A private key and a corresponding public key are generated within a display apparatus. (Block 30 in FIG. 2; page 4, lines 10-19.) The private key is securely stored within the display apparatus such that the private key is inaccessible from outside the display apparatus. The public key is communicated from the display apparatus to an encryption apparatus (Blocks 32 and 34 in FIG. 2; page 4, lines 16-17.). The visual data is encrypted at the encryption apparatus using the public key, whereby encrypted visual data is formed, and the encrypted visual data is transported from the encryption apparatus to the display apparatus. (Blocks 22, 24 and 26 in FIG. 1; page 3, lines 17 to page 4, line 2.) The encrypted visual data is decrypted within the display apparatus such that an electronic version of the visual data is maintained within integrated circuits that are substantially inaccessible, wherein the integrated circuits comprise a decryption integrated circuit and a display integrated circuit (Blocks 38 and 40 in FIG. 3; page 4, lines 20-30), and further wherein, in order to pass the visual data from the decryption integrated circuit to the display integrated circuit, the decryption integrated circuit encodes the visual data and the display integrated circuit decodes the visual data. (Page 4, line 31 through page 5, line 6.) Finally, the visual data is displayed as a visual image. (Page 8, lines 18-27.)

Independent claim 19 relates to a system for securely transmitting and displaying visual data, including an encryption apparatus, means for transporting, and a display apparatus. (Blocks 22, 24 and 26 in FIG. 1; page 3, lines 17 to page 4, line 2.) The encryption apparatus encrypts the visual data, whereby encrypted visual data is formed, and the means for transporting transports the encrypted visual data from the encryption apparatus to a display facility. (Blocks 22, 24 and 26 in FIG. 1; page 3, lines 17 to page 4, line 2.) The display apparatus is located at the display facility that receives the encrypted visual data, and the display apparatus decrypts the encrypted visual data such that an electronic version of the visual data is maintained within integrated circuits that are substantially inaccessible and that the visual data is encoded before being passed between the integrated circuits. (Blocks 38 and 40 in FIG. 3; page 4, lines 20-30; and page 4, line 31 through page 5, line 6.) The display apparatus displays the visual data as

a visual image. (Page 8, lines 18-27.) The encryption apparatus uses a public key for encrypting the visual data, and the display apparatus uses a private key for decrypting the visual data, the private key being generated within and securely residing within the display apparatus so as to be inaccessible from outside the display apparatus. (Block 30 in FIG. 2; page 4, lines 10-19.)

Independent claim 35 relates to a display apparatus for displaying encrypted visual data comprising circuit elements that are substantially inaccessible. (Block 30 in FIG. 2; page 4, lines 10-19.) The circuit elements include a decryption circuit for decrypting the encrypted visual data, whereby visual data is formed, and a display circuit for displaying the visual data as a visual image, such that an electronic version of the visual data is maintained within the circuit elements. (Blocks 38 and 40 in FIG. 3; page 4, lines 20-30.) The display apparatus uses a private key for decrypting the encrypted visual data, wherein the private key is generated within and securely resides within the display apparatus such that the private key is inaccessible from outside the display apparatus, and the encrypted visual data is generated outside the display apparatus using a public key corresponding to the private key. (Blocks 30, 32 and 34 in FIG. 2; page 4, lines 10-19.) The visual data is encoded prior to passing between the circuit elements of the display apparatus. (Page 4, line 31 through page 5, line 6.)

Independent claim 38 relates to a display apparatus for displaying encrypted visual data. A decryption circuit decrypts the encrypted visual data, whereby the visual data is formed, and a display circuit includes a diffractive light valve for displaying the visual data as a visual image. (Blocks 38 and 40 in FIG. 3; page 4, lines 20-30.) The display apparatus uses a private key for decrypting the encrypted visual data, and the private key is generated within and securely resides within the display apparatus such that the private key is inaccessible from outside the display apparatus. The encrypted visual data is generated outside the display apparatus using a public key corresponding to the private key. (Blocks 30, 32 and 34 in FIG. 2; page 4, lines 10-19.) The visual data is encoded prior to passing the visual data from the decryption circuit to the display circuit. (Page 4, line 31 through page 5, line 6.)

Applicants respectfully submit that independent claims 1, 35 and 38 do not include any means-plus-function or step-plus-function elements under the sixth paragraph of 35 U.S.C. § 112.

Independent claim 19 recites a means for transporting. The means for transporting corresponds to the data network 24 in FIG. 1 and the description relating thereto on page 3, line 32 through page 4, line 2, which recites, "The data network 24 is any type of computer data network suitable for transmitting the encrypted digital reproduction including an optical network, a satellite transmission network, or an internet type network."

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following grounds of rejection are to be reviewed on appeal:

1. The rejection of claims 1, 19, 35, 36 and 38 under 35 U.S.C. §103(a) as being unpatentable over Morley et al. (WO 99/59355) in view of Yoshiura et al. (US 6,499,105) and Redmond (US 7,301,944).

2. The rejection of claims 4, 7-8, 10-14, 25-30 and 37 under 35 U.S.C. §103(a) as being unpatentable over Morley et al. (WO 99/59355) in view of Yoshiura et al. (US 6,499,105) and Redmond (US 7,301,944) and further in view of Kowarz et al (US 2002/0113860).

VII. ARGUMENT

Applicants respectfully traverse the aforementioned rejection of claims 1-29 in the latest office action for the following reasons.

A. *Claims 1, 4, 7-8, and 10-14*

Claim 1 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Morley et al. (WO 99/59355) in view of Yoshiura et al. (US 6,499,105) and Redmond (US 7,301,944). Claims 4, 7-8 and 10-14 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Morley et al. (WO 99/59355) in view of Yoshiura et al. (US

6,499,105) and Redmond (US 7,301,944) and further in view of Kowarz et al (US 2002/0113860). These rejections are respectfully traversed.

Claim 1 recites as follows:

1.   A method of securely displaying visual data comprising the steps of:

generating a private key and a corresponding public key within a display apparatus;

securely storing the private key within the display apparatus such that the private key is inaccessible from outside the display apparatus;

communicating the public key from the display apparatus to an encryption apparatus;

encrypting the visual data at the encryption apparatus using the public key, whereby encrypted visual data is formed;

transporting the encrypted visual data from the encryption apparatus to the display apparatus;

decrypting the encrypted visual data within the display apparatus such that an electronic version of the visual data is maintained within integrated circuits that are substantially inaccessible, wherein the integrated circuits comprise a decryption integrated circuit and a display integrated circuit, and further wherein, in order to pass the visual data from the decryption integrated circuit to the display integrated circuit, the decryption integrated circuit encodes the visual data and the display integrated circuit decodes the visual data; and

displaying the visual data as a visual image.

(Emphasis added.)

As shown above, the method of claim 1 recites that "… **an electronic version of the visual data is maintained within integrated circuits that are substantially inaccessible, wherein the integrated circuits comprise a decryption integrated circuit and a display integrated circuit, and further wherein, in order to pass the visual data from the decryption integrated circuit to the display integrated circuit, the decryption integrated circuit encodes the visual data and the display integrated circuit decodes the visual data.**" (Emphasis added.) Advantageously, as discussed in the present application, this claim element avoids the visual data being available as "in-

6

the-clear" data within the display apparatus and prevents a "zealous technician" from being able to easily access an electronic form of the visual data within the display apparatus.

Applicants respectfully submit that the aforementioned claim element is <u>not</u> disclosed or taught by Morley et al., Yoshiura et al., and Redmond, either individually or in combination.

Regarding Morley et al., the latest office action states that "Morley does not specifically disclose the decryption integrated circuit encodes the visual data and the display integrated circuit decodes the visual data." Applicants agree that Morley does <u>not</u> disclose or suggest the above-discussed claim element.

Yoshiura et al. is cited in relation to public and private keys, not the above-discussed claim element. Applicants respectfully submit that there has been no showing that Yoshiura et al. discloses or suggest the above-discussed claim element.

In regard to Redmond, the latest office action cites to col. 10, lines 9-20 in relation to the above-discussed claim element and states that the "copy protection generator is part of decryption integrated circuit." Applicants respectfully <u>disagree</u> with the contention that Redmond discloses the above-discussed claim element.

Applicants respectfully submit the citation to Redmond does <u>not</u> support the contention that it discloses "**decrypting the encrypted visual data within the display apparatus such that an electronic version of the visual data is maintained within integrated circuits that are substantially inaccessible, wherein <u>the integrated circuits comprise a decryption integrated circuit and a display integrated circuit, and further wherein, in order to pass the visual data from the decryption integrated circuit to the display integrated circuit, the decryption integrated circuit encodes the visual data and the display integrated circuit decodes the visual data</u>**." (Emphasis added.)

For convenience of reference, column 10, lines 9-20 and Figure 5 of Redmond are reproduced below.

> Preferably, copy protection generator 76 is a digital signal processing that encodes the media file with analog copy protection. Analog copy protection includes coding that is generated within the data file that inhibits the file from

7

being transferred to another medium, for example, video cassette, by ensuring that any such copy is significantly degraded in quality. Copy protection hardware, such as provided by Macrovision®, include appropriate coding for a given media file type to be displayed in a preselected format (e.g., VGA, HDTV format, NTSC format, etc.).
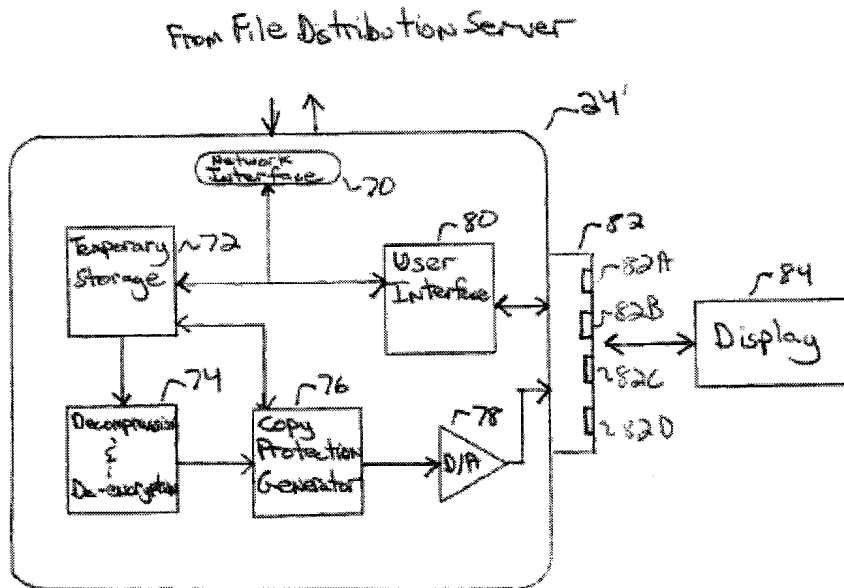

From File Distribution Server

Figure 5

The Examiner contends that the "copy protection generator 76 is part of the display integrated circuit". (Latest office action, bottom of page 3.) Applicants respectfully disagree with this contention.

Applicants respectfully submit that a display integrated circuit is not disclosed or suggested in the above FIG. 5 of Redmond, nor is a display integrated circuit disclosed or suggested in column 10, lines 9-20 of Redmond. The Examiner appears to be contending that block 24' reads on the claimed "display integrated circuit." However, **Redmond clearly describes block 24' as a "media file playback system" and gives the example of a "set-top" system.** (Col. 9, lines 9-17.) As is common knowledge in the art, **a set-top system is not an integrated circuit.** Moreover, FIG. 5 of Redmond clearly shows that the **system 24' is separate from the display 84.**

Therefore, for at least the above-discussed reasons, applicants respectfully submit that the cited references, either individually or in combination, do not disclose or teach claim 1. Hence, applicants respectfully submit that claim 1 overcomes its rejection.

Claims 4, 7-8, 10-14 depend from claim 1. Hence, these claims overcome their rejection for at least the reasons discussed above in relation to claim 1.

B. *Claims 19 and 25-30*

Claim 19 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Morley et al. (WO 99/59355) in view of Yoshiura et al. (US 6,499,105) and Redmond (US 7,301,944). Claims 25-30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Morley et al. (WO 99/59355) in view of Yoshiura et al. (US 6,499,105) and Redmond (US 7,301,944) and further in view of Kowarz et al (US 2002/0113860). These rejections are respectfully traversed.

Claim 19 recites, "the display apparatus decrypting the encrypted visual data such that an electronic version of the visual data is maintained within integrated circuits that are substantially inaccessible and that the visual data is encoded before being passed between the integrated circuits." Applicants respectfully submit that the aforementioned claim element is <u>not</u> disclosed or taught by Morley et al., Yoshiura et al., and Redmond, either individually or in combination.

Regarding Morley et al., the latest office action states that "Morley does not specifically disclose the decryption integrated circuit encodes the visual data and the display integrated circuit decodes the visual data." Applicants agree that Morley does <u>not</u> disclose or suggest the above-discussed claim element.

Yoshiura et al. is cited in relation to public and private keys, not the above-discussed claim element. Applicants respectfully submit that there has been no showing that Yoshiura et al. discloses or suggest the above-discussed claim element.

In regard to Redmond, applicants respectfully submit the citation to Redmond does <u>not</u> disclose the claim language of "the display apparatus decrypting the encrypted visual data such that an electronic version of the visual data is maintained within integrated circuits that are substantially inaccessible and that the visual data is encoded before being passed between the integrated circuits." In

particular, **integrated circuits in a display apparatus are <u>not</u> disclosed or suggested in the above FIG. 5 of Redmond, <u>nor</u> are integrated circuits in a display apparatus disclosed or suggested in column 10, lines 9-20 of Redmond**. The Examiner may contend that copy protector generator 76 in block 24' is an integrated circuit in a display apparatus. However, Redmond clearly shows that the **system 24' is <u>separate</u> from the display 84**.

Therefore, for at least the above-discussed reasons, applicants respectfully submit that the cited references, either individually or in combination, do not disclose or teach claim 19. Hence, applicants respectfully submit that claim 19 overcomes its rejection.

Claims 25-30 depend from claim 19. Hence, these claims overcome their rejection for at least the reasons discussed above in relation to claim 19.

C.   *Claims 35-37*

Claims 35 and 36 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Morley et al. (WO 99/59355) in view of Yoshiura et al. (US 6,499,105) and Redmond (US 7,301,944). Claim 37 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Morley et al. (WO 99/59355) in view of Yoshiura et al. (US 6,499,105) and Redmond (US 7,301,944) and further in view of Kowarz et al (US 2002/0113860). These rejections are respectfully traversed.

Claim 35 recites, "the visual data is encoded prior to passing between the circuit elements of the display apparatus." Applicants respectfully submit that the aforementioned claim element is <u>not</u> disclosed or taught by Morley et al., Yoshiura et al., and Redmond, either individually or in combination.

Regarding Morley et al., the latest office action states that "Morley does not specifically disclose the decryption integrated circuit encodes the visual data and the display integrated circuit decodes the visual data." Applicants agree that Morley does <u>not</u> disclose or suggest the above-discussed claim element.

Yoshiura et al. is cited in relation to public and private keys, not the above-discussed claim element. Applicants respectfully submit that there has been no showing that Yoshiura et al. discloses or suggest the above-discussed claim element.

In regard to Redmond, applicants respectfully submit that the citation to Redmond does **not** disclose the claim language that "the visual data is encoded prior to passing between the circuit elements of the display apparatus." In particular, circuit elements of a display apparatus are **not** disclosed or suggested in FIG. 5 of Redmond, **nor** are circuit elements of a display apparatus disclosed or suggested in **column 10, lines 9-20 of Redmond.** The Examiner may contend that copy protector generator 76 in block 24' is a circuit element in a display apparatus. However, Redmond clearly teaches that the **system 24' is separate from the display 84.**

Therefore, for at least the above-discussed reasons, applicants respectfully submit that the cited references, either individually or in combination, do not disclose or teach claim 35. Hence, applicants respectfully submit that claim 35 overcomes its rejection.

Claims 36-37 depend from claim 35. Hence, these claims overcome their rejection for at least the reasons discussed above in relation to claim 35.

D. *Claim 38*

Claim 38 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Morley et al. (WO 99/59355) in view of Yoshiura et al. (US 6,499,105) and Redmond (US 7,301,944). This rejections is respectfully traversed.

Claim 35 recites, "A display apparatus for displaying encrypted visual data comprising: a decryption circuit for decrypting the encrypted visual data, whereby the visual data is formed; and a display circuit including a diffractive light valve for displaying the visual data as a visual image ...." Applicants respectfully submit that the aforementioned claim language is **not** disclosed or taught by Morley et al., Yoshiura et al., and Redmond, either individually or in combination.

Regarding Morley et al., the latest office action states that "Morley does not specifically disclose the decryption integrated circuit encodes the visual data and the display integrated circuit decodes the visual data." Applicants agree that Morley does **not** disclose or suggest the above-discussed claim element.

Yoshiura et al. is cited in relation to public and private keys, not the above-discussed claim element. Applicants respectfully submit that there has been no showing that Yoshiura et al. discloses or suggest the above-discussed claim element.

In regard to Redmond, applicants respectfully submit that the citation to Redmond does **not** discloses the claim language of "A display apparatus for displaying encrypted visual data comprising: a decryption circuit for decrypting the encrypted visual data, whereby the visual data is formed; and a display circuit including a diffractive light valve for displaying the visual data as a visual image ...." In particular, a display apparatus including the above-claimed decryption and display circuits is **not** disclosed or suggested in FIG. 5 of Redmond, **nor** is such a display apparatus including the above-claimed decryption and display circuits disclosed or suggested in column 10, lines 9-20 of Redmond. The Examiner may contend that copy protector generator 76 in block 24' is a decryption circuit in a display apparatus. However, Redmond clearly teaches that the **system 24' is separate from the display 84**.

Therefore, for at least the above-discussed reasons, applicants respectfully submit that the cited references, either individually or in combination, do not disclose or teach claim 38. Hence, applicants respectfully submit that claim 38 overcomes its rejection.

VIII.   CONCLUSION

        For at least the above reasons, applicants respectfully request that the rejections of

the pendingclaims be overturned.

                                                    Respectfully submitted,
                                                    ROBERT CORRIGAN AND PAUL
                                                    ALIOSHIN

Dated: July 21, 2008   /James K. Okamoto, Reg. No. 40,110/
                                                     James K. Okamoto, Reg. No. 40,110
                                                    Okamoto & Benedicto LLP
                                                    P.O. Box 641330
                                                    San Jose, CA 95164
                                                    Tel.: (408)436-2110
                                                    Fax.: (408)436-2114

CLAIMS APPENDIX

CLAIMS INVOLVED IN THE APPEAL

1.   A method of securely displaying visual data comprising the steps of:

        generating a private key and a corresponding public key within a display apparatus;

        securely storing the private key within the display apparatus such that the private key is inaccessible from outside the display apparatus;

        communicating the public key from the display apparatus to an encryption apparatus;

        encrypting the visual data at the encryption apparatus using the public key, whereby encrypted visual data is formed;

        transporting the encrypted visual data from the encryption apparatus to the display apparatus;

        decrypting the encrypted visual data within the display apparatus such that an electronic version of the visual data is maintained within integrated circuits that are substantially inaccessible, wherein the integrated circuits comprise a decryption integrated circuit and a display integrated circuit, and further wherein, in order to pass the visual data from the decryption integrated circuit to the display integrated circuit, the decryption integrated circuit encodes the visual data and the display integrated circuit decodes the visual data; and

        displaying the visual data as a visual image.

4.   The method of claim 1 wherein displaying the visual data as a visual image comprises:

generating red, green and blue light;

combining the red, green and blue light using a prism;

forming a wedge focused light using a compound lens so as to illuminate an array of controllable light modulating elements;

controlling the light modulating elements using the visual data;

projecting modulated light onto a scanning mirror; and

scanning the modulated light across a display screen using the scanning mirror.

7.   The method of claim 1 wherein the display integrated circuit comprises a driver circuit for driving a diffractive light valve.

8.   The method of claim 1 wherein the step of displaying the visual data comprises scanning a line image over a display screen such that the visual image has low persistence.

10.   The method of claim 1 wherein the step of transporting the encrypted visual data comprises electronic transmission.

11.   The method of claim 10 wherein the electronic transmission is selected from the group consisting of satellite transmission, optical fiber transmission, and internet transmission.

12.   The method of claim 1 wherein the step of transporting the encrypted visual data comprises recording the encrypted visual data on a storage medium and physically transporting the storage medium.

13.   The method of claim 12 wherein the storage medium comprises a standard storage medium.

14.   The method of claim 12 wherein the storage medium comprises a non-standard storage medium.

19.   A system for securely transmitting and displaying visual data comprising:

        an encryption apparatus for encrypting the visual data, whereby encrypted visual data is formed;

        means for transporting the encrypted visual data from the encryption apparatus to a display facility; and

a display apparatus located at the display facility that receives the encrypted visual data, the display apparatus decrypting the encrypted visual data such that an electronic version of the visual data is maintained within integrated circuits that are substantially inaccessible and that the visual data is encoded before being passed between the integrated circuits, the display apparatus displaying the visual data as a visual image,

wherein the encryption apparatus uses a public key for encrypting the visual data, and

wherein the display apparatus uses a private key for decrypting the visual data, the private key being generated within and securely residing within the display apparatus so as to be inaccessible from outside the display apparatus.

25. The system of claim 19 wherein the display apparatus includes a scanning device for scanning a linear image over a display screen such that the visual image has low persistence.

26. The system of claim 19 wherein the means for transporting the encrypted visual data includes means for electronic transmission.

27. The system of claim 26 wherein the means for electronic transmission is selected from the group consisting of satellite transmission, optical fiber transmission, and internet transmission.

28.   The system of claim 19 wherein the means for transporting the encrypted visual data includes a storage medium, the storage medium holding the encrypted visual data during transport of the storage medium.

29.   The system of claim 28 wherein the storage medium comprises a standard storage medium.

30.   The system of claim 28 wherein the storage medium comprises a non-standard storage medium.

35.   A display apparatus for displaying encrypted visual data comprising circuit elements that are substantially inaccessible, the circuit elements comprising a decryption circuit for decrypting the encrypted visual data, whereby visual data is formed, the circuit elements comprising a display circuit for displaying the visual data as a visual image, such that an electronic version of the visual data is maintained within the circuit elements, wherein the display apparatus uses a private key for decrypting the encrypted visual data, wherein the private key is generated within and securely resides within the display apparatus such that the private key is inaccessible from outside the display apparatus, wherein the encrypted visual data is generated outside the display apparatus using a public key

corresponding to the private key, and wherein the visual data is encoded prior to passing between the circuit elements of the display apparatus.

36. The display apparatus of claim 35 wherein the display circuit comprises a diffractive light valve for displaying the visual image.

37. The display apparatus of claim 36 wherein the diffractive light valve is a grating light valve.

38. A display apparatus for displaying encrypted visual data comprising:

a decryption circuit for decrypting the encrypted visual data, whereby the visual data is formed; and

a display circuit including a diffractive light valve for displaying the visual data as a visual image,

wherein the display apparatus uses a private key for decrypting the encrypted visual data,

wherein the private key is generated within and securely resides within the display apparatus such that the private key is inaccessible from outside the display apparatus,

wherein the encrypted visual data is generated outside the display apparatus using a public key corresponding to the private key, and

wherein the visual data is encoded prior to passing the visual data from the decryption circuit to the display circuit.

EVIDENCE APPENDIX

There are no documents or items submitted under this section.

RELATED PROCEEDINGS APPENDIX

There are no documents or items submitted under this section.